

A Note On the Bounds for the Generalized Fibonacci-p-Sequence and its Application in Data-Hiding

Sandipan Dey

Microsoft India Development Center
sandipan.dey@gmail.com

Hameed Al-Qaheri

Department of Quantitative Methods and Information Systems
College of Business Administration
Kuwait University
alqaheri@cba.edu.kw

Suneeta Sane

Computer and Information Technology Department
Veermata Jijabai Technological Institute
Mumbai, Maharashtra 400019, India
sssane@vjti.org.in

Sugata Sanyal

School of Technology and Computer Science
Tata Institute of Fundamental Research
Homi Bhabha Road, Mumbai - 400005, India
sanyal@tifr.res.in
July 2008

In this paper, we suggest a lower and an upper bound for the Generalized Fibonacci-p-Sequence, for different values of p . The Fibonacci-p-Sequence is a generalization of the Classical Fibonacci Sequence. We first show that the ratio of two consecutive terms in generalized Fibonacci sequence converges to a p -degree polynomial and then use this result to prove the bounds for generalized Fibonacci-p sequence, thereby generalizing the exponential bounds for classical Fibonacci Sequence. Then we show how these results can be used to prove efficiency for data hiding techniques using generalized Fibonacci sequence. These steganographic techniques use generalized Fibonacci-p-Sequence for increasing the number of available bit-planes to hide data, so that more and more data can be hidden into the higher bit-planes of any pixel without causing much distortion of the cover image. This bound can be used as a theoretical proof for efficiency of those techniques, for instance it explains why more and more data can be hidden into the higher bit-planes of a pixel, without causing considerable decrease in PSNR.

Keywords: Fibonacci-sequence, LSB Data-hiding, PSNR

1. Introduction

Among many different data hiding techniques proposed to embed secret message within images, the LSB data hiding technique is one of the simplest methods for inserting data into digital signals in noise free environments, which merely embeds secret message-bits in a subset of the LSB planes of the image. (LSB is the least significant bit or the 0th bit, the second LSB is the 1st bit, and so on). Despite

being simple, this technique is more predictable and hence less secure, also PSNR (peak signal to noise ratio) decreases very rapidly as we use the higher bit planes for data hiding. As soon as we go from LSB (least significant bit) to MSB (most significant bit) for selection of bit-planes for our message embedding, the distortion in stego-image is likely to increase exponentially, so it becomes impossible (without noticeable distortion and with exponentially increasing distance from cover-image and stego-image) to use higher bit-planes for embedding without any further processing. The workarounds may be: through the random LSB replacement (in stead of sequential), secret messages can be randomly scattered in stego-images, so the security can be improved. Also, using the approaches given by variable depth LSB algorithm [Liu *et al.* (2004)], or by the optimal substitution process based on genetic algorithm and local pixel adjustment [Wang *et al.* (2001)], one is able to hide data to some extent in higher bit-planes as well.

Battisti *et al.* [Battisti *et al.* (2006)], [Picione *et al.* (2006)] proposed a novel data hiding technique from a totally different perspective, it uses a different bit-planes decomposition altogether, based on the generalized Fibonacci-p-sequences, that not only increases the number of embeddable bit-planes but also decreases PSNR in the stego image considerably, thereby improving the LSB technique. In this paper, we first prove some theoretical upper and lower bounds for generalized Fibonacci-p-sequence and give a theoretical proof for the better performance of the data hiding technique using generalized Fibonacci decomposition, i.e., why the data hiding technique using this decomposition not only gives larger number of bit planes for hiding secret bits, but also gives a far better PSNR than that in classical LSB technique.

The Generalized Fibonacci-p-Sequence ([Horadam (1961)], [Basin and Hoggatt (1963)], [Hoggatt (1972)], [Atkins and Geist (1987)], [Hendel (1994)], [Sun and Sun (1992)]) is given by,

$$\begin{aligned} F_p(0) &= F_p(1) = \dots = F_p(p) = 1, \\ F_p(n) &= F_p(n-1) + F_p(n-p-1), \quad \forall n \geq p+1, \quad n, p \in \mathbb{N} \end{aligned} \quad (1)$$

For $p = 1$, we have,

$$\begin{aligned} F(0) &= F(1) = 1, \\ F(n) &= F(n-1) + F(n-1), \quad \forall n \geq 2, \quad n \in \mathbb{N} \end{aligned}$$

We get the classical Fibonacci sequence $1, 1, 2, 3, 5, 8, \dots$. We already have some results for this Classical Fibonacci Sequence, e.g., we know the ratio of two consecutive terms in Fibonacci sequence converge to Golden Ratio, $\frac{1+\sqrt{5}}{2}$. In this paper, we show that $\alpha_p^n > F_p(n) > \alpha_p^{n-p}$, $\forall n, p \in \mathbb{N}$, where α_p is the positive Root of $x^{p+1} - x^p - 1 = 0$. The ratio of two consecutive terms in Fibonacci-p-Sequence converges to this α_p .

2. Bounds for the generalized Fibonacci-p-Sequence

In this section we prove the upper and lower bounds for the generalized Fibonacci-p-sequence. First, we show that the ratio of consecutive terms of generalized Fibonacci-p-sequence converges to the positive root of the polynomial $x^{p+1} - x^p - 1 = 0$. Next we use this root to prove a bound on the generalized Fibonacci-p-sequence.

2.1. Lemma 1

The ratio of two consecutive numbers in generalized Fibonacci p-sequence converges to the positive root of the degree- p polynomial $P(x) = x^{p+1} - x^p - 1$.

Proof:

Convergence

Let us first define the ratio of two consecutive terms of Fibonacci-p-sequence as a sequence $\{\beta_n\} = \left\{ \frac{F_p(n+1)}{F_p(n)} \right\}$.

Now, by definition of Fibonacci-p-sequence, we have

$$\begin{aligned} \beta_0 &= \beta_1 = \dots = \beta_p = 1 \\ \beta_n &= 1 + \frac{F_p(n-p)}{F_p(n)} > 1, \forall n > p \\ \beta_{p+1} &= \beta_p + \beta_0 = 1 + 1 = 2 \\ \beta_n &= 1 + \frac{F_p(n-p)}{F_p(n)} < 1 + 1 = 2, \forall n > p+1 \\ &\Rightarrow 1 < \beta_n < 2, \forall n > p+1 \end{aligned}$$

We observe that the sequence β_n is bounded and hence by Monotone Convergence theorem must have a convergent subsequence. For instance, for $p = 1$ (classical Fibonacci sequence), we have two convergent subsequences β_{2n} (increasing) and β_{2n+1} (decreasing), $n \in \mathbb{N}$ (natural number) and they both converge to the same limit $\frac{1+\sqrt{5}}{2} \approx 1.618$ [Craw (2000)], as shown in figure 2.

Positive Root of the polynomial $x^{p+1} - x^p - 1$

Now, let's analyze the polynomial function $y = P(x) = x^{p+1} - x^p - 1$. By Descartes' rule, the polynomial can have at most one positive real root, since it has exactly one change in sign.

First we observe that the function $P(x)$ is continuous and differentiable everywhere. We also notice that the function has exactly one positive root α_p (and α_p is also strictly larger than 1). This is a consequence of elementary calculus. By successive differentiation, we see that

$$y_1 = P'(x) = (p+1)x^p - px^{p-1}$$

$$y_2 = P''(x) = (p+1)px^{p-1} - p(p-1)x^{p-2}$$

- The function $P(x)$ has critical points at $P'(x) = 0$, i.e., at $x = 0$ and $x = \frac{p}{p+1}$.
- $y_2 \Big|_{x=\frac{p}{p+1}} = \frac{p^{p-1}}{(p+1)^{p-2}} > 0, \forall p \geq 1$.
- By 2nd order sufficient condition for local minima, $P(x)$ has a (local) minima at $x = \frac{p}{p+1}$.
- At $x = 0$, the function will have a maxima or a point of inflection depending on whether p is odd or even, explained in the next section.

When $p \in \mathbb{N}_{odd}$, we have,

$$y_1 = P'(x) = (p+1)x^{p-1} \left(x - \frac{p}{p+1} \right) \text{ is } \begin{cases} < 0 & x < 0 \\ = 0 & x = 0 \\ < 0 & 0 < x < \frac{p}{p+1} \\ = 0 & x = \frac{p}{p+1} \\ > 0 & x > \frac{p}{p+1} \end{cases}$$

Hence the function is decreasing in $(-\infty, \frac{p}{p+1})$ and increasing in $(\frac{p}{p+1}, \infty)$. Also, $y(-1) = 1$, $y(0) = y(1) = -1$ and $y(2) = 2^p - 1 \geq 1, \forall p \in \mathbb{N}_{odd}$. At $x = \frac{p}{p+1}$, $P(x)$ has a minima (gradient changes from *negative* to *positive*) but at $x = 0$ (no sign change in gradient) we have a point of inflection. Again, $P(x)$ being a continuous function assumes all possible values within an interval. Combining all these, we can easily see that the graph of the function has exactly two real zeroes, one positive and the other negative (the remaining roots are complex conjugate pairs).

When $p \in \mathbb{N}_{even}$, we have,

$$y_1 = P'(x) = (p+1)x^{p-1} \left(x - \frac{p}{p+1} \right) \text{ is } \begin{pmatrix} > 0 & x < 0 \\ = 0 & x = 0 \\ < 0 & 0 < x < \frac{p}{p+1} \\ = 0 & x = \frac{p}{p+1} \\ > 0 & x > \frac{p}{p+1} \end{pmatrix}$$

Hence the function is increasing in $(-\infty, 0)$, then decreasing in $(0, \frac{p}{p+1})$ and again increasing in $(\frac{p}{p+1}, \infty)$. Also, $y(-1) = y(0) = y(1) = -1$ and $y(2) = 2^p - 1 \geq 1, \forall p \in \mathbb{N}_{even}$. At $x_0 = \frac{p}{p+1}$, $P(x)$ has a minima but at $x = 0$ (gradient changes from *positive* to *negative*) we have a maxima. Combining all these, we can easily see that we have exactly one real (positive) root at α_p , since $y(1) < 0$ and $y(2) > 0$, also $y(x)$ being continuous. (From this result we immediately have Lemma 2). From figure 1 we can see the graph of the degree- p polynomial, for odd and even p respectively.

Convergence to the positive root of the polynomial

Now, we show that if sequence $\{\beta_n\}$ converges to β , then $\beta = \alpha_p$.

Let's assume the sequence $\{\beta_n\}$ converges to $\beta \in \mathbb{R}^+$. Now we prove, the sequence must converge to the only positive root α_p of the above-stated p -degree polynomial. By assumption,

$$\begin{aligned}
 \beta &= \lim_{n \rightarrow \infty} \left(\frac{f_{n+p}}{f_{n+p-1}} \right) = \lim_{n \rightarrow \infty} \left(\frac{f_{n+p-1}}{f_n} \right) = \dots = \lim_{n \rightarrow \infty} \left(\frac{f_n}{f_{n-1}} \right) = \dots, \\
 f_n &= n^{\text{th}} \text{ number in the Fibonacci-} p \text{ Sequence, } f_{n+p} = f_{n+p-1} + f_{n-1} \\
 &\Rightarrow \beta = \lim_{n \rightarrow \infty} \left(\frac{f_{n+p-1} + f_{n-1}}{f_{n+p-1}} \right) = \lim_{n \rightarrow \infty} \left(\frac{f_n}{f_{n-1}} \right), \\
 &\Rightarrow \beta = 1 + \lim_{n \rightarrow \infty} \prod_{k=n-1}^{k=n+p-2} \left(\frac{f_k}{f_{k+1}} \right) = \lim_{n \rightarrow \infty} \left(\frac{f_n}{f_{n-1}} \right) \\
 &\Rightarrow \beta = 1 + \prod_{k=1}^{k=p} \left(\frac{1}{\beta} \right) \Rightarrow \beta = 1 + \frac{1}{\beta^p} \\
 &\Rightarrow \beta^{p+1} - \beta^p - 1 = 0
 \end{aligned}$$

Hence β satisfies the equation $x^{p+1} - x^p - 1 = 0$, $\forall p \in \mathbb{N}$, $\beta \in \mathbb{R}^+$, i.e., from above results, we have, $\beta = \alpha_p$

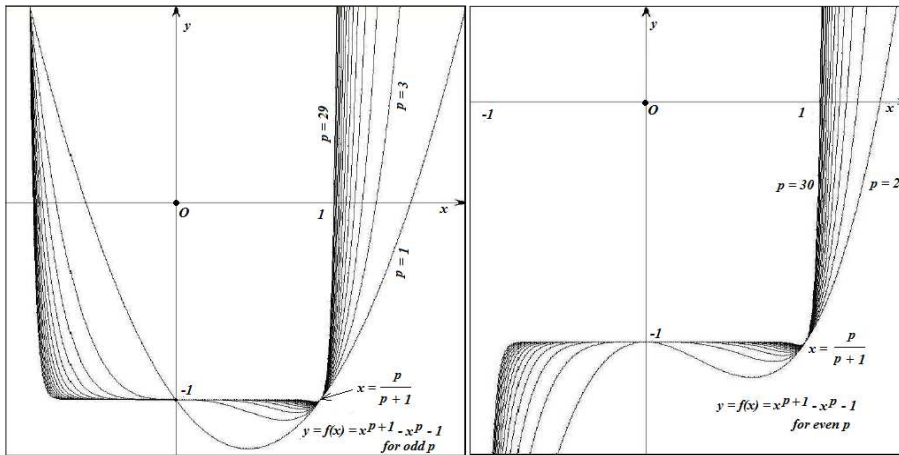


Fig. 1. Graph of $x^{p+1} - x^p - 1 = 0$, showing α_p for different values of p

2.2. Lemma 2

If α_p be a positive root of the equation $x^{p+1} - x^p - 1 = 0$, we have $1 < \alpha_p < 2$, $\forall p \in \mathbb{N}$.

Proof: We have,

$$\begin{aligned}
 & \alpha_p^{p+1} - \alpha_p^p - 1 = 0 \\
 \text{Also, } & 2^{p+1} - 2^p - 1 = 2^p - 1 > 0, \forall p \in \mathbb{N} \\
 & \Rightarrow 2^p - 1 > \alpha_p^{p+1} - \alpha_p^p - 1 \\
 & \Rightarrow (2^p - \alpha_p^p) > \alpha_p^p(\alpha_p - 2) \tag{2}
 \end{aligned}$$

Also,

$$\begin{aligned}
 -1 < 0 &= \alpha_p^{p+1} - \alpha_p^p - 1 \\
 &\Rightarrow \alpha_p^p(\alpha_p - 1) > 0 \\
 &\Rightarrow \alpha_p > 1 \text{ (since positive)} \tag{3}
 \end{aligned}$$

From (2), we immediately see the following:

- $\alpha_p > 0$ according to our assumption, hence we can not have $\alpha_p = 2$ (LHS & RHS both becomes 0, that does not satisfy inequality (2)).
- If $\alpha_p > 2$, we have LHS < 0 while RHS > 0 which again does not satisfy inequality (2).
- Hence we have $\alpha_p < 2$, $\forall p \in \mathbb{N}$

From (3), we have, $\alpha_p > 1$. Combining, we get, $1 < \alpha_p < 2$, $\forall p \in \mathbb{N}$

2.3. Lemma 3

If α_p be a positive root of the equation $x^{p+1} - x^p - 1 = 0$, where $p \in \mathbb{N}$, we have the following results, $\forall k \in \mathbb{N}$,

- $\alpha_k > \alpha_{k+1}$
- $\lim_{k \rightarrow \infty} \alpha_k = 1$
- $\alpha_{k+1} > \frac{1+\alpha_k}{2}$
- $\alpha_k^k < (k+1)$
- $\alpha_k^{k+1} > 1$

Proof: We have,

$$\begin{aligned}
 & \text{For } p = k, \alpha_k^{k+1} - \alpha_k^k - 1 = 0 \\
 & \text{For } p = k+1, \alpha_{k+1}^{k+2} - \alpha_{k+1}^{k+1} - 1 = 0 \\
 & \Rightarrow \alpha_{k+1}^{k+1}(\alpha_{k+1} - 1) = \alpha_k^k(\alpha_k - 1) \\
 & \Rightarrow \left(\frac{\alpha_k}{\alpha_{k+1}} \right)^k = \left(\frac{\alpha_{k+1} - 1}{\alpha_k - 1} \right) \cdot \alpha_{k+1} \tag{4}
 \end{aligned}$$

From (4) we can argue,

- $\alpha_k \neq \alpha_{k+1}$, since neither of them is 0 or 1 (from Lemma 2).
- If $\alpha_k < \alpha_{k+1}$, we have LHS of inequality (4) < 1 , but RHS > 1 , since both the terms in RHS will be greater than 1 (by our assumption and by Lemma 2), a contradiction.
- Hence we must have

$$\alpha_k > \alpha_{k+1}, \forall k \in \mathbb{N} \quad (5)$$

Also, from Lemma 2, we have, $1 < \alpha_k < 2, \forall k \in \mathbb{N}$.

Hence we have,

$$\begin{aligned} 2 > \alpha_1 > \alpha_2 > \dots > \alpha_k > \alpha_{k+1} > \dots > 1, \quad k \in \mathbb{N} \\ \Rightarrow \lim_{k \rightarrow \infty} \alpha_k = 1 \end{aligned}$$

Again, from (4) we have,

$$\begin{aligned} \Rightarrow \left(\frac{\alpha_{k+1} - 1}{\alpha_k - 1} \right) \cdot \alpha_{k+1} > 1, \text{ since } \left(\frac{\alpha_k}{\alpha_{k+1}} \right)^k > 1, \text{ from (5)} \\ \Rightarrow 2 > \alpha_{k+1} > \left(\frac{\alpha_k - 1}{\alpha_{k+1} - 1} \right), \text{ (from Lemma 2)} \\ \Rightarrow \alpha_{k+1} > \frac{1 + \alpha_k}{2} \end{aligned} \quad (6)$$

Now, let us induct on $p \in \mathbb{N}$ to prove $\alpha_p^p < p + 1$.

Base case:

For $p = 1$, $1 < \alpha_1 < 2$, by Lemma 2.

Let us assume the inequality holds $\forall p \leq k \Rightarrow p < \alpha_p^p < p + 1, \forall p \leq k$

Induction Step:

$$\begin{aligned} p = k + 1, \quad \alpha_{k+1}^{k+1} &= \alpha_k^k \cdot \left(\frac{\alpha_k - 1}{\alpha_{k+1} - 1} \right), \text{ by (4)} \\ &\Rightarrow \alpha_{k+1}^{k+1} < (k + 1) \cdot \left(\frac{\alpha_k - 1}{\alpha_{k+1} - 1} \right) \\ k < \alpha_k^k < k + 1, \text{ by induction hypothesis} \\ &\Rightarrow \alpha_{k+1}^{k+1} < (k + 1) \cdot \left(1 + \frac{\alpha_k - \alpha_{k+1}}{\alpha_{k+1} - 1} \right) \\ &\Rightarrow \alpha_{k+1}^{k+1} < (k + 1) + \left(\frac{\alpha_k - \alpha_{k+1}}{\alpha_{k+1} - 1} \right) \\ &\Rightarrow \alpha_{k+1}^{k+1} < (k + 1) + 1, \left(\text{from (6), we have, } \frac{\alpha_k - \alpha_{k+1}}{\alpha_{k+1} - 1} < 1 \right) \\ &\Rightarrow \alpha_{k+1}^{k+1} < (k + 2) \\ &\Rightarrow \alpha_p^p < (p + 1), \forall p \in \mathbb{N} \end{aligned} \quad (7)$$

Also, since α_p is a root of $x^{p+1} - x^p - 1 = 0$, for $p = k$ we have.

$$\begin{aligned} \alpha_k^{k+1} - \alpha_k^k - 1 &= 0 \\ \Rightarrow \alpha_k^{k+1} &= \alpha_k^k + 1 > 1 + 1 \quad (\text{since from Lemma 2, we have, } \alpha_k > 1) \\ &\Rightarrow \alpha_k^{k+1} > 2 \end{aligned} \quad (8)$$

2.4. Lemma 4

The following inequalities always hold:

- $(k+1)^{\frac{1}{k}} < k^{\frac{1}{k-1}} < \dots < 4^{\frac{1}{3}} < 3^{\frac{1}{2}} < 2$
- $\alpha_p^p < p+1 \Rightarrow \alpha_p^{p-1} < p \Rightarrow \dots \alpha_p^3 < 4 \Rightarrow \alpha_p^2 < 3 \Rightarrow \alpha_p < 2$
- $\alpha_p^{p+2} > 2 \Rightarrow \alpha_p^{p+3} > 3 \Rightarrow \dots \alpha_p^{p+p} > p \Rightarrow \alpha_p^{p+p+1} > p+1$

Proof: By Binomial Theorem, we have,

$$\begin{aligned} (k+1)^{k-1} &= \sum_{r=0}^{k-1} \frac{(k-1)(k-2)\dots(k-r)}{r!} . k^{k-1-r} \\ &= \sum_{r=0}^{k-1} \frac{(1-\frac{1}{k})(1-\frac{2}{k})\dots(1-\frac{r}{k})}{r!} . k^{k-1} = \sum_{r=0}^{k-1} \frac{\prod_{s=1}^r (1-\frac{s}{k})}{r!} . k^{k-1} \\ &< \underbrace{(1+1+1+\dots+1)}_{k \text{ times}} . k^{k-1} = k . k^{k-1} = k^k \Rightarrow (k+1)^{\frac{1}{k}} < k^{\frac{1}{k-1}} \end{aligned} \quad (9)$$

Hence we have, $(k+1)^{\frac{1}{k}} < k^{\frac{1}{k-1}} < \dots < 4^{\frac{1}{3}} < 3^{\frac{1}{2}} < 2$

Also, from (7) we have, $\alpha_k < (k+1)^{\frac{1}{k}}$.

Combining, we get,

$$\begin{aligned} \alpha_k &< (k+1)^{\frac{1}{k}} < k^{\frac{1}{k-1}} < \dots < 4^{\frac{1}{3}} < 3^{\frac{1}{2}} < 2 \\ \alpha_k^k &< (k+1) \Rightarrow \alpha_k^{k-1} < k \dots \Rightarrow \alpha_k^4 < 5 \Rightarrow \alpha_k^3 < 4 \Rightarrow \alpha_k^2 < 3 \Rightarrow \alpha_k < 2 \end{aligned} \quad (10)$$

Also, we have,

$$\begin{aligned} \alpha_k^{k+1} &> 2 \Rightarrow \alpha_k^{k+2} = \alpha_k^{k+1} + \alpha_k > 2 + 1 = 3 \\ \alpha_k^{k+2} &> 3 \Rightarrow \alpha_k^{k+3} = \alpha_k^{k+2} + \alpha_k^2 > 3 + 1 = 4 \\ \Rightarrow \alpha_p^{p+2} &> 2 \Rightarrow \alpha_p^{p+3} > 3 \Rightarrow \dots \alpha_p^{p+p} > p \Rightarrow \alpha_p^{p+p+1} > p+1 \end{aligned} \quad (11)$$

2.5. Lemma 5

The following inequality gives us the lower and upper bounds for generalized Fibonacci-p-sequence,

$$\alpha_p^n > F_p(n) > \alpha_p^{n-p}, \quad \forall n > p, \quad n \in \mathbb{N} \quad (12)$$

where α_p is the *positive* root of the equation $x^{p+1} - x^p - 1 = 0$.

Proof: We induct on n to show the result.

$$F_p(0) = F_p(1) = \dots = F_p(p) = 1, \text{ (By definition of Fibonacci-p-Sequence).}$$

Base case:

From Lemma 4, we have,

$$\begin{aligned} \alpha_p^{p+1} &> F_p(p+1) = F_p(p) + F_p(0) = 1 + 1 = 2 > \alpha_p \\ \alpha_p^{p+2} &> F_p(p+2) = F_p(p+1) + F_p(1) = 2 + 1 = 3 > \alpha_p^2 \\ \alpha_p^{p+3} &> F_p(p+3) = F_p(p+2) + F_p(2) = 3 + 1 = 4 > \alpha_p^3 \\ &\dots \quad \dots \quad \dots \\ \alpha_p^{p+p+1} &> F_p(p+p+1) = F_p(p+p) + F_p(p) = (p+1) + 1 = p+2 > \alpha_p^{p+1} \end{aligned}$$

Induction Step:

Let's assume the above result is also true $\forall m : (2p+1 < m < n), m, n \in \mathbb{N}$.

Now, we prove for $m = n$,

$$\begin{aligned} \alpha_p^{n-1} + \alpha_p^{n-p-1} &> F_p(n-1) + F_p(n-p-1) \text{ (by hypothesis)} \\ F_p(n-1) + F_p(n-p-1) &> \alpha_p^{n-p-1} + \alpha_p^{n-2p-1} \text{ (by hypothesis)} \\ &\Rightarrow \alpha_p^{n-p-1} \cdot (1 + \alpha_p^p) > F_p(n) > \alpha_p^{n-2p-1} \cdot (1 + \alpha_p^p) \\ &\Rightarrow \alpha_p^{n-p-1} \cdot \alpha_p^{p+1} > F_p(n) > \alpha_p^{n-2p-1} \cdot \alpha_p^{p+1} \\ &\Rightarrow \alpha_p^n > F_p(n) > \alpha_p^{n-p}, \forall n > p, n \in \mathbb{N} \end{aligned}$$

Hence we have the following inequality,

$$(\alpha_p)^n > F_p(n) > (\alpha_p)^{n-p}, \alpha_p \in \mathbb{R}^+ \text{ and } \alpha_p \in (1, 2) \quad (13)$$

$$\alpha_1 = \frac{1 + \sqrt{5}}{2} \approx 1.618034,$$

$$\alpha_2 \approx 1.465575,$$

$$\alpha_3 \approx 1.380278,$$

$$\alpha_4 \approx 1.324718,$$

$$\alpha_p > \alpha_{p+1}, \forall p \in \mathbb{N}$$

The empirical results (Table 1) also prove our claim for $p = 2$.

Also $F_p(0) = F_p(1) = \dots = F_p(p) = 1$ and $F_p(n+1) > F_p(n), \forall n > p$. Hence we have,

$$\begin{aligned} F_p(n) &= F_p(n-1) + F_p(n-p-1) < 2.F_p(n-1), \forall n > p \\ \Rightarrow F_p(n) &< 2.F_p(n-1) < 2^2.F_p(n-2) < \dots < 2^{n-p}.F_p(p) = 2^{n-p}, \forall n > p \\ &\Rightarrow F_p(n) < 2^{n-p}, \forall n > p \quad (14) \end{aligned}$$

n	α_2^n	$Fib_2(n)$	α_2^{n-2}
3	3.148	2	1.466
4	4.614	3	2.148
5	6.761	4	3.148
6	9.909	6	4.613
7	14.523	9	6.761
8	21.285	13	9.909
9	31.194	19	14.523
10	45.717	28	21.284
11	67.002	41	31.193
12	98.197	60	45.716
13	143.915	88	67.000
14	210.918	129	98.194
15	309.115	189	143.910
16	453.032	277	210.910
17	663.952	406	309.104
18	973.072	595	453.013
19	1426.110	872	663.923

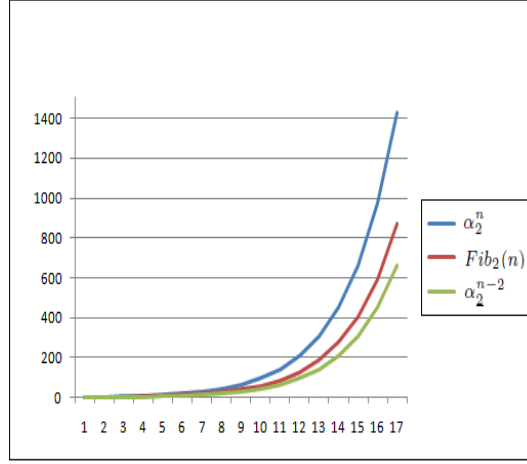


Table 1

α_2 is a *positive* Root of $x^3 - x^2 - 1 = 0$, $\alpha_2 \approx 1.465571$, with $\alpha_2^n > F_2(n) > \alpha_2^{n-2}$

Combining (13) and (14), we have,

$$(2)^{n-p} > F_p(n) > (\alpha_p)^{n-p}, \forall n > p, \text{ and } n, p \in \mathbb{N} \quad (15)$$

where α_p is the positive Root of $x^{p+1} - x^p - 1 = 0$.

Figure 2 and Table 2 show the convergence of ratio of successive terms for Fibonacci-p-sequences for different p (For $p = 1$ we get classical Fibonacci sequence). It can be noticed that smaller the value of p , quicker the convergence of the ratio is achieved, as shown. Also value to which the ratio converges monotonically decreases with increase in the value of p .

3. Application in Data Hiding

Data hiding is a new kind of secret communication technology, where message is hidden inside an image or any other medium, so that it cannot be observed. One of the simplest data hiding technique is LSB data hiding technique, which merely embeds secret message-bits in a subset of the LSB planes of the image. One of the drawbacks of this technique is: as soon as we go from LSB to MSB for selection of bit-planes for our message embedding, the distortion in stego-image is likely to increase exponentially, so it becomes impossible (without noticeable distortion and with exponentially increasing distance from cover-image and stego-image) to use higher bit-planes for embedding without any further processing.

This particular problem was addressed by Battisti *et al.*, [Battisti *et al.* (2006)], who proposed to use generalized Fibonacci-p-sequence decomposition technique instead of classical binary decomposition and shows by empirical results that this

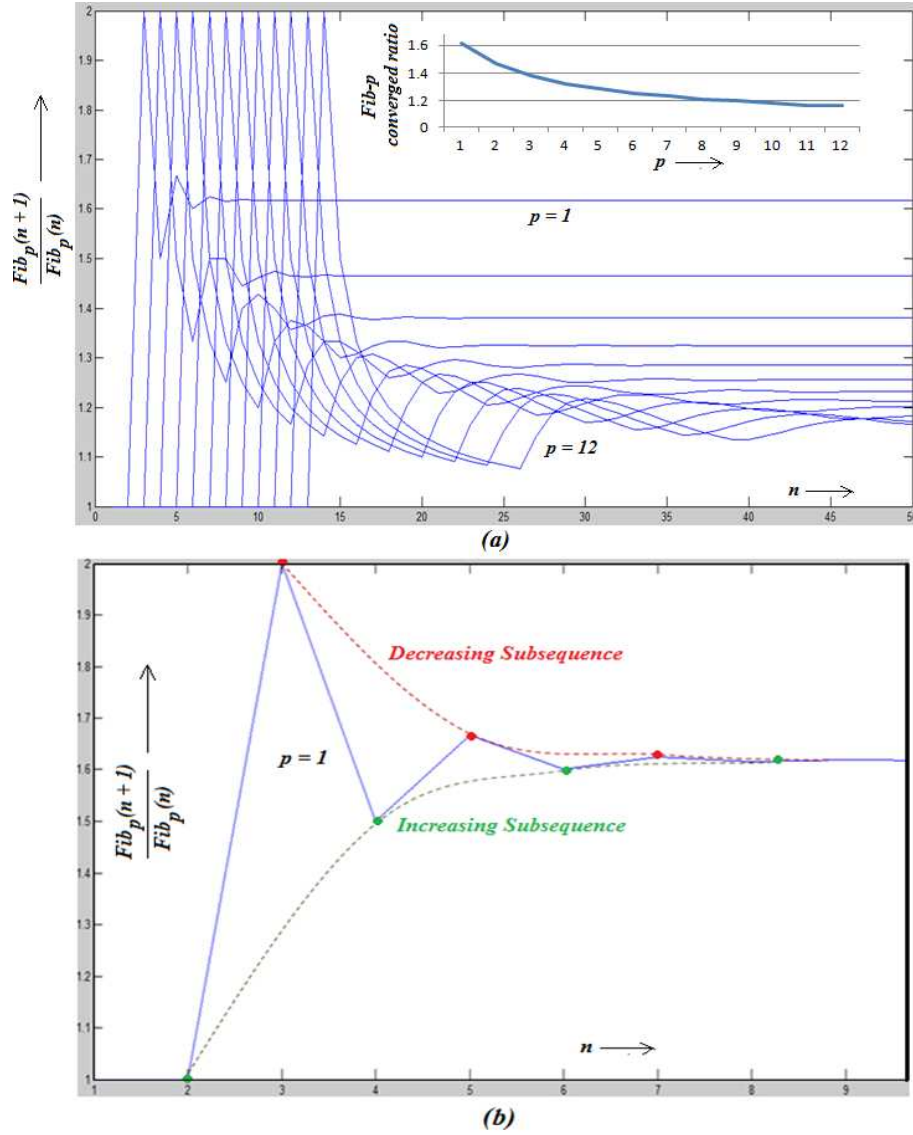


Fig. 2. (a) Convergence of the ratio of successive terms in generalized Fibonacci p-Sequence for different values of p (b) Convergent Subsequences for classical Fibonacci sequence ($p=1$)

technique outperforms the classical LSB technique when thought in terms of embedding in the higher bit plane as well with less distortion. This technique basically increases the number of bit-planes (by generating a new larger set of bit-planes that we call virtual bit-planes) by using Fibonacci-p-sequence decomposition. It can be further improved using prime and natural number decomposition techniques

n	$\frac{f_1(n)}{f_1(n-1)}$	$\frac{f_2(n)}{f_2(n-1)}$	$\frac{f_3(n)}{f_3(n-1)}$	$\frac{f_4(n)}{f_4(n-1)}$	$\frac{f_5(n)}{f_5(n-1)}$
1	1.000000	1.000000	1.000000	1.000000	1.000000
2	2.000000	1.000000	1.000000	1.000000	1.000000
3	1.500000	2.000000	1.000000	1.000000	1.000000
4	1.666667	1.500000	2.000000	1.000000	1.000000
5	1.600000	1.333333	1.500000	2.000000	1.000000
6	1.625000	1.500000	1.333333	1.500000	2.000000
7	1.615385	1.500000	1.250000	1.333333	1.500000
8	1.619048	1.444444	1.400000	1.250000	1.333333
9	1.617647	1.461538	1.428571	1.200000	1.250000
10	1.618182	1.473684	1.400000	1.333333	1.200000
11	1.617978	1.464286	1.357143	1.375000	1.166667
12	1.618056	1.463415	1.368421	1.363636	1.285714
13	1.618026	1.466667	1.384615	1.333333	1.333333
14	1.618037	1.465909	1.388889	1.300000	1.333333
15	1.618033	1.465116	1.380000	1.307692	1.312500
16	1.618034	1.465608	1.376812	1.323529	1.285714
17	1.618034	1.465704	1.378947	1.333333	1.269259
18	1.618034	1.465517	1.381679	1.333333	1.264706
19	1.618034	1.465546	1.381215	1.325000	1.279070
20	1.618034	1.465596	1.380000	1.320755	1.290909
21	1.618034	1.465571	1.379710	1.321429	1.295775
22	1.618034	1.465563	1.380252	1.324324	1.293478
23	1.618034	1.465574	1.380518	1.326531	1.285714
24	1.618034	1.465573	1.380375	1.326154	1.281046
25	1.618034	1.465570	1.380192	1.324826	1.280612
26	1.618034	1.465571	1.380208	1.323993	1.282869
27	1.618034	1.465572	1.380294	1.324074	1.285714
28	1.618034	1.465571	1.380316	1.324675	1.287440
29	1.618034	1.465571	1.380282	1.325038	1.287054
30	1.618034	1.465571	1.380261	1.324986	1.285714
31	1.618034	1.465571	1.380270	1.324742	1.284580
32	1.618034	1.465571	1.380283	1.324578	1.284201
33	1.618034	1.465571	1.380283	1.324602	1.284536
34	1.618034	1.465571	1.380277	1.324709	1.285179
35	1.618034	1.465571	1.380275	1.324777	1.285595
36	1.618034	1.465571	1.380277	1.324768	1.285622
37	1.618034	1.465571	1.380279	1.324722	1.285390
38	1.618034	1.465571	1.380278	1.324692	1.285126
39	1.618034	1.465571	1.380277	1.324697	1.284995
40	1.618034	1.465571	1.380277	1.324716	1.285036
41	1.618034	1.465571	1.380278	1.324729	1.285160
42	1.618034	1.465571	1.380278	1.324727	1.285263
43	1.618034	1.465571	1.380278	1.324719	1.285291
44	1.618034	1.465571	1.380277	1.324713	1.285254
45	1.618034	1.465571	1.380278	1.324714	1.285197
46	1.618034	1.465571	1.380278	1.324718	1.285161
47	1.618034	1.465571	1.380278	1.324720	1.285161
48	1.618034	1.465571	1.380278	1.324720	1.285184
49	1.618034	1.465571	1.380278	1.324718	1.285207
50	1.618034	1.465571	1.380278	1.324717	1.285218
51	1.618034	1.465571	1.380278	1.324717	1.285213
52	1.618034	1.465571	1.380278	1.324718	1.285202
53	1.618034	1.465571	1.380278	1.324718	1.285193

Table 2
Convergence of the ratio of consecutive terms of Fibonacci-p-Sequences
for different values of p (p = 1, 2, 3, 4, 5)

as shown in [Dey *et al.* (2007a)], [Dey *et al.* (2007b)], [Dey *et al.* (2008)]. Also, [Cooper (1984)] [Dotson *et al.* (1993)] illustrates Fibonacci sequence can be used in various applications.

In this paper we give a formal proof of Fibonacci-p-sequence bounds and show how this can be used to theoretically prove that Fibonacci-p-sequence decomposition gives better result in hiding data. From (15) it is clear (from the upper bound) that the same value will require more numbers of bits to be represented than the number of bits required in classical binary decomposition (since $2^n > \alpha^n > F_p n$), if it's expressed using Fibonacci-p-sequence decomposition (where the radix is Fibonacci-p-sequence numbers instead of powers of 2).

As illustrated in [Dey *et al.* (2008)], in order to measure the distortion in the stego-image, we use Mean square error (MSE), Worst case Mean Square Error

(WMSE) and Peak Signal to Noise Ratio (PSNR), which are defined by

$$MSE = \sum_{i=1}^M \sum_{j=1}^N (f_{ij} - g_{ij})^2 / MN$$

$$PSNR = 10 \cdot \log_{10} \left(\frac{L^2}{MSE} \right)$$

[Dey *et al.* (2008)]. If the secret data-bit is embedded in the i^{th} bit-plane of a pixel, the worst-case error-square-per-pixel will be $= WSE = |W(i)(1..0)|^2 = (W(i))^2$ (here $W(i)$ represents the corresponding weight in the number system for the i^{th} bit, e.g., for classical decomposition $W(i) = 2^i$, for generalized Fibonacci decomposition $W(i) = F_p i$), corresponding to the case when the corresponding bit in cover-image toggles in stego-image, after embedding the secret data-bit. For example, worst-case error-square-per-pixel for embedding a secret data-bit in the i th bit plane in case of a pixel in classical binary decomposition is $= (2^i)^2 = 4^i$, where $i \in \mathbb{N} \cup \{0\}$. If the original k -bit grayscale cover-image has size $w \times h$, we define, $WMSE = w \times h \times (W(i))^2 = w \times h \times WSE$ [Dey *et al.* (2008)]. Hence,

WMSE after embedding secret message bit only in the l^{th} (virtual) bit-plane of each pixel in case of classical (traditional) binary (LSB) data hiding technique is given by,

$$(WMSE_{l^{th} \text{ bit-plane}})_{\text{Classical-Binary-Decomposition}} = \theta(4^l).$$

WMSE after embedding secret message bit in the l^{th} (virtual) bit-plane of each pixel in case of generalized Fibonacci decomposition is given by,

$$(WMSE_{l^{th} \text{ bit-plane}})_{\text{Fibonacci-p-Sequence Decomposition}} = (F_p(l))^2$$

$$\Rightarrow (\alpha_p^2)^{l-p} < (WMSE_l)_{\text{Fibonacci-p-sequence}} < (\alpha_p^2)^l,$$

$$\alpha_p \in \mathbb{R}^+, \alpha_1 = \frac{1 + \sqrt{5}}{2},$$

$$\alpha_p^2 > \alpha_{p+1}^2, \forall p \in \mathbb{N}, \alpha_1^2 \approx 2.618,$$

$$\Rightarrow (WMSE_l)_{\text{Generalized-Fibonacci-p-sequence}} < \theta(2.618^l).$$

Hence, we have,

$$(WMSE)_{\text{Binary}} > (WMSE)_{\text{Fibonacci}}$$

$$\Rightarrow (PSNR)_{\text{Fibonacci}} > (PSNR)_{\text{Binary}}.$$

Thus, we have first proved bounds on the generalized Fibonacci sequence and then by using our bounds, we have given a formal proof for better performance (in terms of PSNR) for LSB data hiding technique using generalized Fibonacci-p-sequence decomposition than that using classical binary decomposition. Also, we

have,

$$\begin{aligned} (\text{number of primes} \leq n) &= p_n = \theta(n \cdot \log n) \\ &= o(\alpha_p)^{n-p} < F_p(n) < 2^{n-p} \end{aligned}$$

([Telang (1999)], [Niven and Zuckerman (1966)], [Tattersall (2005)])

The above implies that if the same number is represented using prime decomposition (n^{th} prime number as weightage to n^{th} bit), it will give still more numbers of virtual bit planes [Battisti *et al.* (2006)].

We have similar results for LSB data hiding using natural number decomposition technique, and combining the results (from [Battisti *et al.* (2006)], [Dey *et al.* (2007a)], [Dey *et al.* (2007b)], [Dey *et al.* (2008)]) we have the following,

$$\begin{aligned} (WMSE)_{\text{Binary}} &> (WMSE)_{\text{Fibonacci}} > (WMSE)_{\text{Prime}} > (WMSE)_{\text{Natural}} \\ \Rightarrow (PSNR)_{\text{Natural}} &> (PSNR)_{\text{Prime}} > (PSNR)_{\text{Fibonacci}} > (PSNR)_{\text{Binary}}. \end{aligned}$$

Hence, data hiding using natural number decomposition gives the best performance among the above mentioned techniques.

In data hiding, we hide data in different bit-planes of a pixel. In classical LSB data-hiding technique the pixel is represented as binary value, hence it has less numbers of bit-planes as we have in case of Fibonacci-p-sequence decomposition, the later having still less number of bit-planes than in case of prime decomposition technique. It is shown in [Dey *et al.* (2007a)], [Dey *et al.* (2007b)], [Dey *et al.* (2008)] by calculation of WMSE and PSNR measures that embedding data even in higher bit-planes of pixel using these techniques results in less visible distortion of the cover image, since the distortion as measured by WMSE is proportional to the square of the weights to the bits in the corresponding decomposition, hence it decreases as the weights go on decreasing from classical binary to generalized Fibonacci and from that to prime and natural number decomposition [Dey *et al.* (2008)].

4. Conclusions

In this paper, we have established the bounds for generalized Fibonacci-sequence $(\alpha)^n > F_p(n) > (\alpha_p)^{n-p}$, $\forall n > p, (n, p) \in \mathbb{N}$. Empirical results obtained vindicates our theoretically-proven bounds. Then we used the result $(2)^{n-p} > F_p(n) > (\alpha_p)^{n-p}$, $\forall n > p, (n, p) \in \mathbb{N}$, where α_p is the positive Root of $x^{p+1} - x^p - 1 = 0$, to prove that data hiding technique using generalized Fibonacci-p-sequence gives more embeddable bit-planes along with better PSNR than that in case of classical LSB technique [Dey *et al.* (2008)], and the same using prime decomposition technique increases virtual bit-planes and PSNR further [Dey *et al.* (2007a)].

References

- Battisti F., Carli M., Neri A., Egiazarian K. (2006). A Generalized Fibonacci LSB Data Hiding Technique. *3rd International Conference on Computers and Devices for Communication (CODEC- 06, December 18–20) TEA*, Institute of Radio Physics and Electronics, University of Calcutta.

- Basin S. L. and Hoggatt V. E. Jr. (1963). A Primer on the Fibonacci Sequence, *Fib. Quart.* 1.
- Atkins J. and Geist R. (1987). Fibonacci numbers and computer algorithms. *College Math. J.* 18, 328–337.
- Cooper C. (1984). Application of a Generalized Fibonacci Sequence. *The College Mathematics Journal*, Vol. 15, 2, 145–148
- Craw I. (2000). *Advanced Calculus and Analysis*, MA1002, Department of Mathematical Sciences, University of Aberdeen, DSN mth200-101982-8, 26–27, V. 1.3.
- Dey S., Abraham A. and Sanyal S. (2007a). An LSB Data Hiding Technique Using Prime Numbers. *Third International Symposium on Information Assurance and Security (IAS 07, August 29–31)*, Manchester, United Kingdom, *IEEE Computer Society press*, USA, ISBN 0-7695-2876-7, 101–106.
- Dey S., Abraham A. and Sanyal S. (2007b). An LSB Data Hiding Technique Using Natural Numbers. *IEEE Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP 07, Nov 26–28)*, Kaohsiung City, Taiwan, *IEEE Computer Society press*, USA, ISBN 0-7695-2994-1, 473–476.
- Dey S., Abraham A., Bandyopadhyay B. and Sanyal S. (2008). Data Hiding Techniques Using Prime and Natural Numbers. *Journal of Digital Information Management*, Vol. 6.
- Dotson W., Norwood F. and Taylor C. (1993). Fiber optics and Fibonacci. *this MAGAZINE* 66, 167–174.
- Hendel R. J. (1994). Approaches to the formula for the n th Fibonacci number, *College Math. J.* 25, 139–142.
- Hoggatt V. E. Jr. (1972). Fibonacci and Lucas numbers. *The Fibonacci Association*, Santa Clara, California, USA.
- Horadam A. (1961). A generalized Fibonacci sequence. *American Mathematical Monthly*, 68, 455–459.
- Liu S. H., Chen T. H., Yao H. X., Gao W. (2004). A Variable Depth LSB Data Hiding Technique in images. *Proceedings of the 3rd International Conference on Machine Learning and Cybernetics, 26-29 August*, Shanghai.
- Niven I. and Zuckerman H. S. (1966). An Introduction to the Theory of Numbers. *Wiley*, 2nd ed., New York.
- Picione D. D. L., Battisti F., Carli M., Astola J. and Egiazarian K. (2006). A Fibonacci LSB data hiding technique. *Proc. European signal processing conference*.
- Sun Z. H. and Sun Z. W. (1992). Fibonacci numbers and Fermat's last theorem. *Acta Arith.* 60, 371–388.
- Tattersall J. J. (2005). Elementary number theory in nine chapters, 2nd ed., *Cambridge University Press*, ISBN 9780521850148, 28–31.
- Telang S. G. (1999). Number Theory. *Tata McGraw-Hill*, ISBN 0-07-462480-6, First Reprint, 617–631.
- Wang R. Z., Lin C. F. and Lin I. C. (2001). Image Hiding by LSB substitution and genetic algorithm. *Pattern Recognition*, Vol. 34, 3, 671–683.